

PP Presentation

PP Presentation

PP Presentation

Probabilistic MaxAgeDiff Attack

Undetected Tampering

Fresher LSA?

Linear Case LSA Age

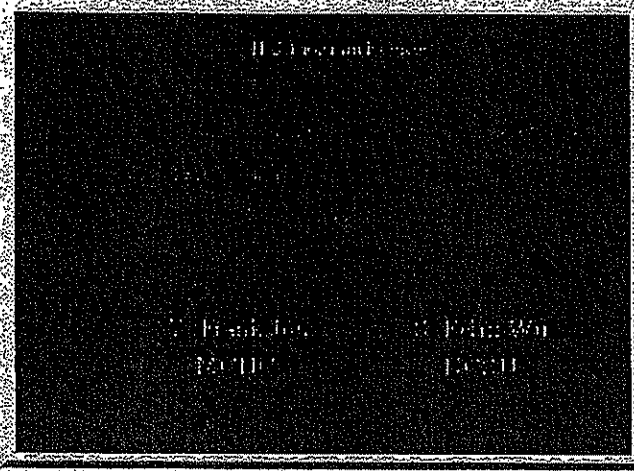
Attacker's (E) Learning Phase

MaxAgeDiff Attack

PP Presentation

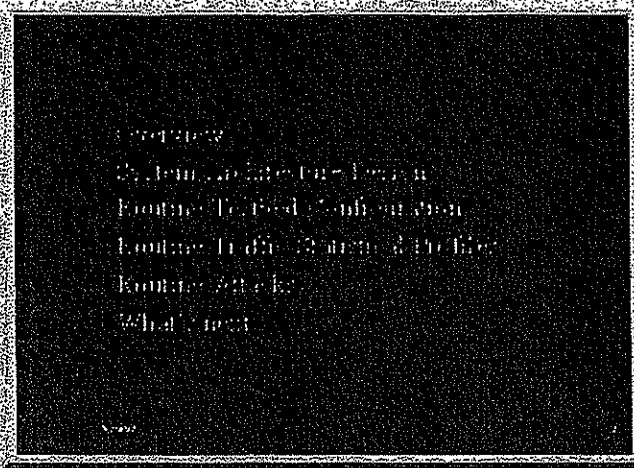
Scalable Intrusion Detection for the Emerging Network Infrastructure

4 of 1



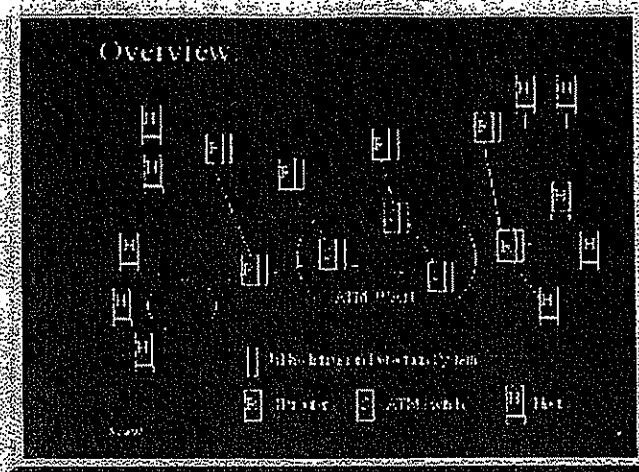
Project Update

1 of 1



PP Presentation

1 of 1



Overview

Interactions of attack prevention,
notification, response, and intrusion
detection

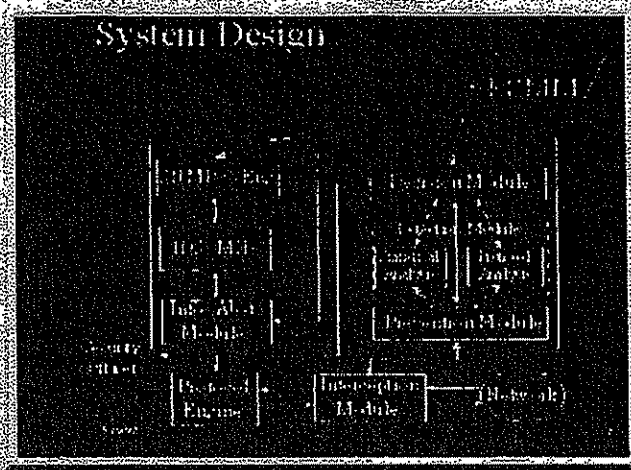
Interactions involving:

- Intrusion Detection System (IDS) or
Intrusion Prevention System (IPS) to
detect and/or prevent attacks and
notify the administrator



System Design:

1 of 1



System Design

- Multiple data multiplexed lanes
- Two channels
- High speed protocols
- Multiple communication direction
- Out of band (e.g. Ethernet, ATM)
- Multiple transport layers



System Design

Prevention Layer (aka: HICU)

Control response

Enforcement Layer

Full form data collection

Multiple intersection point correlation

e.g. Traffic Management Plan team (downtown and
suburban)



System Design

1. Maintain a set of Finite State Machines
2. Use FSMs to describe functions in
the system architecture
3. Use a set of FSMs to describe
the system architecture
4. Use a set of FSMs to describe
the system architecture
5. Use a set of FSMs to describe
the system architecture



System Design

Data can be used in different ways

- Complementing to rule-based and protocol-based analysis

Profile analysis

- Comparing short-term to long-term behaviors

- Weighted sums for time series comparison

- Supplementing with ML or statistical analysis

